

(S//SI//REL) What Your Mother Never Told You About SIGDEV Analysis



SSG21 Net Pursuit
Network Analysis Center

Derived From: NSA/CSSM 1-52
Dated: 20070108
Declassify On: 20370401



(U//FOUO) What have I learned in my first two years in **SIGDEV**....

- ☞ (U//FOUO) Important to understand the data that you are searching against
- ☞ (S//SI//REL) Important to understand the hidden treasures and nuances in various SIGDEV tools
- ☞ (U//FOUO) Nothing is 100%: there are always exceptions to the tools and the rules
- ☞ (S//SI//REL) Took a network view of VPNs

(TS//SI//REL)What Makes SIGDEV Analysis Challenging?

- (U//FOUO) Requires knowledge of.....
 - ⇒ (S//SI//REL) Access and collection
 - ⇒ (S//SI//REL) Network protocols
 - ⇒ (S//SI//REL) Routing
 - ⇒ (TS//SI//REL) Encryption

(U//FOUO) Challenges etc....

(TS//SI//REL) Technical jargon and abbreviations

- ⇒ IPSEC
- ⇒ IKE
- ⇒ MPLS
- ⇒ PSK
- ⇒ PPTP
- ⇒ L2TP
- ⇒ GRE
- ⇒ Cisco commands

(TS//SI//REL)Challenges etc....

(S//SI//REL) Tools

- ⇒ How to use them
- ⇒ Knowing that they exist
- ⇒ Multiple query languages
- ⇒ SQL for TOYGRIPPE
- ⇒ Oracle Text Query in DISCOROUTE
- ⇒ Quantity

(U//FOUO) Tools

- „ DISCOROUTE
- „ BLACKPEARL
- „ TOYGRIPPE
- „ GNETWORK GNOME
- „ NKB & RONIN
- „ XKEYSCORE
- „ TREASUREMAP
- „ RENOIR
- „and more....

(S//SI//REL) Building Network Knowledge

BLACKPEARL

TOYGRIPPE

XKEYSCORE

Maximize the overlap of the tools for success

(S//SI//REL)

DISCOROUTE

NAC's router configuration database

(U//FOUO) DISCORUTE

- ⇒ (C) NAC project to acquire, parse, database and display configuration files from network devices
- ⇒ (C) Allows analysts to mine device configs for SIGDEV discovery

Router configs are a rich source
of
network and VPN information

(S//SI//REL) DISCORUTE

Methodology

(S//SI//REL) All IPs are important because they all belong to a device and they all have a purpose in the network

- ⇒ (S//SI//REL) Search for
 - ⇒ Endpoint IPs
 - ⇒ Loopback IPs
 - ⇒ Opposite end of a point-to-point connection
 - ⇒ IPs found in pings and telnets
- ⇒ (S//SI//REL) Make note of the source and destination IPs of the config

(U//FOUO) DISCOROUTE Searches

- (U//FOUO) Country
- (U//FOUO) IP Search
- (U//FOUO) Text Query
- (TS//SI//REL) Manifest Tag Selection
 - K - Crypto Keys
 - H - TAO Pop
 - M - Multihop
- (S//SI//REL) VPN report



(S//SI//REL) DISCOROUTE: Country Search

- (S//SI//REL) IPGeo lookup on every IP address that is parsed
- (S//SI//REL) Configs with only private IPs will not show up in the results of a country search

(S//SI//REL) DISCOROUTE: Searching for IP

- ⇒ (S//SI//REL) Text **Addressess** query IP search
 - ⇒ searches through the payload
 - ⇒ If you only search using this field, then you will miss configs that have your IPs of interest as the source and destination address
 - ⇒ configs where your IP falls within the range of the interface mask
- ⇒ (S//SI//REL) IP address field search
 - ⇒ searches through the parsed file
 - ⇒ If you only search using this field, then you will miss configs with your IPs of interest in pings, telnets, arp commands

(S//SI//REL) DISCOROUTE Search 1Feb to 13 Apr:

- ⇒ (S//SI//REL) T [REDACTED] in the payload
 - ⇒ 3 results
- ⇒ (S//SI//REL) IP Address Search: searching for the IP in the parsed file
 - ⇒ Exact IP search
 - ⇒ De-duped by most recent
 - ⇒ 28 results (27 had [REDACTED] as the source IP)
- ⇒ (S//SI//REL) Somalia Country search: 66 results
(12 of those had a source IP of [REDACTED])
- ⇒ (S//SI//REL) Difference: IP was the source IP for configs more times than it occurred in the payload data



(S//SI//REL) Why fewer configs for
[REDACTED] in the country
search?

- ☞ (S//SI//REL) 12 as opposed to 27
- ☞ (S//SI//REL) Geo location for [REDACTED]
was Hong Kong for a period of time
- ☞ (S//SI//REL) Geo is assigned to router configs
at the time of ingest and not changed if the IP
location is corrected

(S//SI//REL) Data Found in a Text Query: Inner Network IPs in a Huawei Config

~~<LNC>~~dis firew se t

04:19:05 2011/06/18

Current total sessions : 19

udp VPN: public -> public

Term	Percentage (%)
Climate change	95
Global warming	92
Green energy	88
Sustainable development	85
Carbon footprint	60
Renewable energy	82
Environmental protection	80
Green economy	84
Eco-friendly	86
Green technology	89

Inner IPs

Press CTRL+K to abort

Connected to [REDACTED] ...



(S//SI//REL) DISCOROUTE Manifest Tag

- » (TS//SI//REL) H - TAO has a presence on the router
- » (S//SI//REL) M - multihop router. The admin telnetted into a router and then telnetted again to another device. Potential goldmine of information about your network, but be careful when looking through them to make sure you are associating an IP with the correct device.
- » (TS//SI//REL) K - crypto keys

(S//SI//REL) VPNs in Router Configs

- ⇒ (TS//SI//REL) DISCOROUTE sets manifest tags to 'K' for configs with crypto information
- ⇒ (S//SI//REL) Separate parsers developed for each vendor to pull out the endpoints and the pre-shared keys
 - ⇒ Cisco
 - ⇒ Huawei
 - ⇒ Juniper

(S//SI//REL) VPN Information in a Cisco

(S//SI//REL) Endpoint Configuration and Description Fields

crypto isakmp key VpnsAreCool address [REDACTED]

```
crypto map VPNS-ROCK 10 ipsec-isakmp  
    set peer [REDACTED]
```

interface Tunnel1

description Tunnel TO theStars

bandwidth 512

ip address [REDACTED]

ip tcp adjust-mss 1350

load-interval 30 keepalive 5 2

tunnel source [REDACTED]

tunnel destination [REDACTED]

crypto map VPNS-ROCK



(S//SI//REL) VPN Information in a

(S//SI//REL) Netstrings: Usernames, SNMP Community &
Cisco Config
Domain Names

Username **deb** privilege 5 password 7
082C495A0C1617

snmp-server community **dancer** RW 70

snmp-server community **tangosnmp** RW 60

ip domain name **lifesabeach**

(S//SI//REL) VPN Information in a Huawei Config

```
# ike proposal 60 authentication-algorithm md5
# ike peer e ---- More ----.[42D .[42D
exchange-mode aggressive pre-shared-key GoHokies
ike-proposal 60
undo version 2
local-id-type name
remote-name svn
remote-address [REDACTED]
remote-address authentication-address [REDACTED]
nat traversal
# ipsec proposal GoHokies
# ipsec policy helloworld 60 isakmp
security acl 3060
ike-peer proposal GoHokies
# interface Virtual-Template1 ---- More ----.[42D .[42D
ip address [REDACTED]
remote address pool 1
# interface GigabitEthernet0/0/0
ip address [REDACTED]
# interface GigabitEthernet0/0/1
description GigabitEthernet0/0/1 Interface
ip address [REDACTED]
ipsec policy helloworld
```

(S//SI//REL) VPN Information in a Juniper Config

```
set ike gateway "BadguyVPN" address [REDACTED] Main outgoing-interface "untrust" preshare  
"xGe7YOYfNx3DNGsp4GCq+fgCdondsCBQtVwo/3YfCvbR7zJyDUewVD4=" proposal "pre-g2-3des-sha" "pre-g2-  
3des-md5"  
set ike gateway "BadguyVPN" cert peer-ca all  
set ike gateway "BadguyVPN Backup" address [REDACTED] Main outgoing-interface "untrust" preshare  
"YWZpKbUvNGQvCbsiXdCwv3pxRDnLEAxo9877SfjFLBgg9utCdSyYPPI=" proposal "pre-g2-3des-sha" "pre-g2-  
3des-md5"  
set ike gateway "To Mouse" address [REDACTED] Main outgoing-interface "untrust" preshare  
"fn3VG5E1NI+amHsDeyChciqYVHnuTsbj4w==" proposal "pre-g2-3des-sha"  
set ike respond-bad-spi 1  
set vpn "BadguyVPN" gateway "BadguyVPN" no-replay tunnel idletime 0 proposal "nopfs-esp-3des-sha"  
set vpn "BadguyVPN" monitor optimized rekey  
set vpn "BadguyVPN" id 5 bind interface tunnel.3  
set vpn "backup BadguyVPN" gateway "BadguyVPN Backup" no-replay tunnel idletime 0 proposal "nopfs-esp-  
3des-sha" "nopfs-esp-3des-sha" "nopfs-esp-3des-sha" "nopfs-esp-3des-md5"  
set vpn "backup BadguyVPN" monitor optimized rekey  
set vpn "backup BadguyVPN" id 4 bind interface tunnel.1  
set vpn "From Rat" gateway "To Mouse" no-replay tunnel idletime 0 proposal "nopfs-esp-des-md5"  
set vpn "From Rat" monitor optimized rekey  
set vpn "From Rat" id 6 bind interface tunnel.2
```

(S//SI//REL) VPN Report Search Fields

- ☞ (S//SI//REL) Some of the fields that you can search in...
 - ☞ Country
 - ☞ IP Address
 - ☞ SIGAD/Case Notation
 - ☞ Descriptions: crypto map and interface
 - ☞ Netstrings: Username, Domain Name
 - ☞ Pre-shared keys
 - ☞ Device Hostname
 - ☞ TAO Project Name

(S//SI//REL) DISCOROUTE VPN

Report

Click to edit Master text styles

Second level

Third level

Fourth level

Fifth level

The screenshot shows a web-based application for managing network knowledge. At the top, there's a navigation bar with links for 'Query', 'Reports' (which is currently selected), 'New!', 'Network Mgmt Query', 'Wiki', and 'Feedback'. To the right of the navigation is the text 'version 2.17' and a link to 'NKB HOME'. Below the navigation is a title bar for 'Discoroute Reports'. Underneath, a 'VPN Report Form' section is visible. This form includes fields for 'Start Date' (set to 2012-03-14 00:00:00) and 'End Date' (set to 2012-04-13 23:59:59). There are three radio button options: 'DOI' (selected), 'Load Date', and 'Entire Database'. To the right of these date fields is a detailed 'IP Address' configuration panel with fields for 'IP Address' (with a placeholder '(1.2.3.4)'), 'Tunnel Source', 'Tunnel Dest', 'Interface', 'VPN Source', and 'VPN Remote'. Below this are sections for 'Hostname', 'SIGAD', 'Case', 'Country', 'TAO Project Name', 'Session ID', 'Pre-Shared Keys', 'Snmp Community', 'Interface Descr', 'Crypto Descr', 'Username', and 'Domain Name'. At the bottom of the report form are buttons for 'Generate Report', 'Generate Report in New Window', and 'Clear Panel'. At the very bottom of the page, there's a footer with the text 'Powered by the SIGDEV Lab', 'Version Number: 2.17 New!', 'Last Modified Date: March 28, 2012', 'Last Reviewed Date: March 28, 2012', 'Content Steward [REDACTED]', and 'Page Publisher: [REDACTED]'. The word 'NAC' is also present in the footer.

Powered by the SIGDEV Lab
Version Number: 2.17 New!
Last Modified Date: March 28, 2012
Last Reviewed Date: March 28, 2012
Content Steward [REDACTED]
Page Publisher: [REDACTED]

NAC

(S//SI//REL) VPN Report

Network Knowledge Base  DiscoRoute

Query Reports  Network Mgmt Query Wiki Feedback

DiscoRoute Reports

VPN Report Form

Query Results

Session ID:1332289408998

Hostname	Vendor	Sigad	Case Notation	Collection Source	Country	TAO Project	TAO Pop
IBL_Baghdad_Router	cisco	USJ-759A	E9BDJ00000M0000	XKeyscore	LB		No

Interfaces

Interface ID	IP Address	Network Mask	Description
Loopback0	[REDACTED]	255.255.255.255	voice traffic
FastEthernet0/0	[REDACTED]	255.255.255.240	Connected To ASA/Firewall
FastEthernet0/1	[REDACTED]	255.255.255.248	Connected To 2MB DSL
Serial0/1/0	[REDACTED]	255.255.255.240	Connected To DVB

Tunnels

ID	Source	Dest	Description
Tunnel1	[REDACTED]	[REDACTED]	Tunnel TO Beirut
Tunnel1	[REDACTED]	[REDACTED]	Tunnel TO Beirut
Tunnel1	[REDACTED]	[REDACTED]	Tunnel TO Beirut
Tunnel1	[REDACTED]	[REDACTED]	Tunnel TO Beirut

VPN Peers

ID	Router IP	Remote IP	VPN Type	PSKs	Description
Serial0/1/0	[REDACTED]	[REDACTED]	ipsec	IblBaghdad	
Tunnel1	[REDACTED]	[REDACTED]	ipsec	IblvoiceVpn	
Serial0/1/0	[REDACTED]	[REDACTED]	ipsec	IblBaghdad	
Tunnel1	[REDACTED]	[REDACTED]	ipsec	IblvoiceVpn	
Serial0/1/0	[REDACTED]	[REDACTED]	ipsec	IblBaghdad	
Tunnel1	[REDACTED]	[REDACTED]	ipsec	IblvoiceVpn	
Serial0/1/0	[REDACTED]	[REDACTED]	ipsec	IblBaghdad	
Tunnel1	[REDACTED]	[REDACTED]	ipsec	IblvoiceVpn	

(S//SI//REL) VPN Report

Hints:

- = (TS//SI//REL) Use the VPN report as a start but not as the final answer for VPNs from a country or a SIGAD
- = (C) Query in different ways to make sure you get as much of the data as possible
- = (TS//SI//REL) Depending on your scenario you may want to start with a country search, an IP range or a descriptive term

VPN Peers Section contains the endpoint IPs for your VPN which can be entered into TOYGRIPPE

(S//SI//REL) Description & Net Strings Searches

- ⇒ (S//SI//REL) Suppose you do a general VPN report query
 - ⇒ Search by country
 - ⇒ Search by SIGAD
- ⇒ (S//SI//REL) Find a VPN of interest
- ⇒ (S//SI//REL) Analyze the NetStrings and the description fields

(S//SI//REL) NetStrings

Examples

- ⇒ (S//SI//REL) Do a follow-on VPN report using a netstring specific to your network
 - ⇒ Snmp community string: pegasus
 - ⇒ Domain name: badguy.com
 - ⇒ Username
- ⇒ (S//SI//REL) Search ROYALNET
 - ⇒ Analytics to find other netstrings related to your target
 - ⇒ Analytics to find links likely to carry your target's communications

(U//FOUO)

BLACKPEARL

(S//SI//REL) NAC tool enabling automated DNI link and network characterization against survey collection across the SIGINT system



(S//SI//REL) BLACKPEARL

Searches

- ⇒ (U//FOUO) General Query
- ⇒ (S//SI//REL) Customized reports
 - ⇒ VPN report
 - ⇒ DNI Access Essentials
 - ⇒ MPLS report
 - ⇒ Five Tuple Report



(S//SI//REL) BLACKPEARL IP

Searches

- ⇒ Endpoint IPs
- ⇒ Interface IPs
- ⇒ Loopback IPs
- ⇒ Source or destination IPs of the router config file
- ⇒ Inner network IPs
- ⇒ Analyze other IPs on the link



(U//FOUO) BLACKPEARL

- ⇒ (S//SI//REL) Search ‘All traffic’ and include subchannels and tunnels if no results found under limited search
- ⇒ (S//SI//REL) If link is identified as MPLS then look at the other IPs in inner labels, if present
- ⇒ (S//SI//REL) Use BLACKPEARL for finding access and gathering information on your network



(S//SI//REL) Search for Inner Tunneled IPs

- ☞ (S//SI//REL) Query BLACKPEARL with an endpoint IP
 - ☞ Find other tunneled IPs – inner network IPs that you can do follow on searches
- ☞ (S//SI//REL) Query DISCROUTE with any new IPs found
- ☞ (TS//SI//REL) Success: Discovered information on Somalia's Hormuud network

(TS//SI//REL) Example: Hormuud Network

- ☞ (S//SI//REL) Began with loopback IPs from a spreadsheet
 - ☞ [REDACTED]
- ☞ (S//SI//REL) Found configs for 2 of the 12 loopbacks in a text query in DISCOROUTE
 - ☞ [REDACTED] and [REDACTED] were in the payload but not parsed
- ☞ (S//SI//REL) Took the IPs from those configs and found other configs, one with hostname 'LNS'

(U) Example continued

⇒ (S//SI//REL) BLACKPEARL hit on LNS IP
[REDACTED]

- ⇒ Inner IPs in L2TP tunnels
- ⇒ DR search for inner IPs from the L2TP tunnels and found more configs
- ⇒ (U//FOUO) Many of the configs were multi-hop
- ⇒ (S//SI//REL) Information compiled for TAO
 - ⇒ ~400 IPs for over 50 devices

(S//SI//REL) BLACKPEARL Search:

L2TP tunnel Number of Five Tuples: 1							
#	Source Address	Dest Address	Source Port	Dest Port	Next Protocol	% Packets	# Pack
1	[REDACTED]	[REDACTED]	22	4527	TCP (6)	100.0	43

L2TP tunnel Number of Five Tuples: 6							
#	Source Address	Dest Address	Source Port	Dest Port	Next Protocol	% Packets	# Pack
1	[REDACTED]	[REDACTED]	9101	53771	TCP (6)	67.2	39
2	[REDACTED]	[REDACTED]	6006	53779	TCP (6)	8.6	5
3	[REDACTED]	[REDACTED]	6000	53050	TCP (6)	6.0	4
4	[REDACTED]	[REDACTED]	6006	53783	TCP (6)	6.9	4
5	[REDACTED]	[REDACTED]	6000	53778	TCP (6)	5.2	3
6	[REDACTED]	[REDACTED]	6000	53782	TCP (6)	5.2	3

L2TP tunnel Number of Five Tuples: 2							
#	Source Address	Dest Address	Source Port	Dest Port	Next Protocol	% Packets	# Pack
1	[REDACTED]	[REDACTED]	23	3078	TCP (6)	83.3	20
2	[REDACTED]	[REDACTED]	23	3080	TCP (6)	16.7	4

Content Steward: [REDACTED] General Support: Contact the Mission Support Team [REDACTED] [Contact Us](#)

SECUR

(S//SI//REL) BLACKPEARL MPLS

6	7938	255			
+ Tuple List (label stack 1046418, 7938):					
7	7211	255			
+ Tuple List (label stack 1046418, 7211):					
8	6660	255			
+ Tuple List (label stack 1046418, 6660):					
9	6306	255			
+ Tuple List (label stack 1046418, 6306):					
	#	Source Address	Dest Address	Protocol Number	Pkt Count
	1	[REDACTED]	[REDACTED]	SIPP-ESP (50)	1
1 of 1					
10	7180	255			
+ Tuple List (label stack 1046418, 7180):					
11	8120	255			
+ Tuple List (label stack 1046418, 8120):					
12	6315	255			
+ Tuple List (label stack 1046418, 6315):					
	#	Source Address	Dest Address	Protocol Number	Pkt Count
	1	[REDACTED]	[REDACTED]	SIPP-ESP (50)	1
	2	[REDACTED]	[REDACTED]	SIPP-ESP (50)	6
	3	[REDACTED]	[REDACTED]	SIPP-ESP (50)	1
	4	[REDACTED]	[REDACTED]	SIPP-ESP (50)	1
4 of 4					
13	6705	255			
+ Tuple List (label stack 1046418, 6705):					

(U//FOUO) TOYGRIPPE

(S//SI//REL) VPN Metadata Repository



(S//SI//REL)Building VPN Network Knowledge

- ⇒ (S//SI//REL)VPNs are part of a larger network
- ⇒ (S//SI//REL)Inner or tunneled IPs are a peek inside the target's network
- ⇒ (S//SI//REL)Beneficial to look beyond the endpoints of your VPN
- ⇒ (S//SI//REL)Combine information from as many SIGDEV databases as you can

(U//FOUO) TOYGRIPPE

Searches

- (U//FOUO) Search 3 months at a time
- (U//FOUO) Keep going back in time if no results found
- (S//SI//REL) Take endpoint IPs found here and search in
 - DISROUTE -- device information
 - BLACKPEARL -- inner tunneled IPs
- (S//SI//REL) Country report



(U//FOUO) TOYGRIPPE

Searches

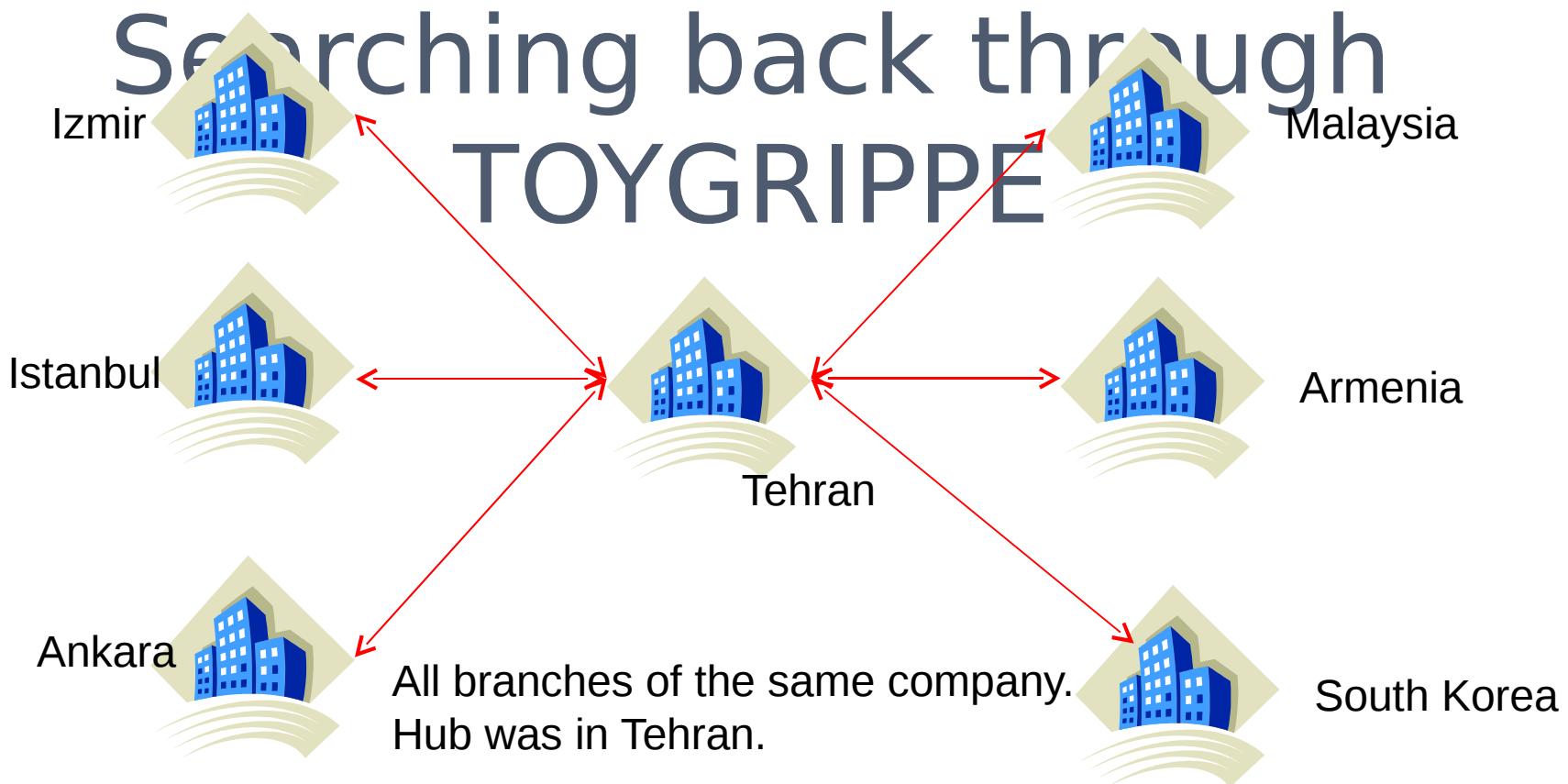
- ☞ (S//SI//REL) Make note of other connections to the IP of interest and search for them separately
- ☞ (S//SI//REL) You might not find what you are looking for, but it still may be important
- ☞ (S//SI//REL) Convert the target domain name to hex and search for it in the idData field
 - ⇒ badguy.com = 6261646775792e636f6d
 - ⇒ (idData LIKE '%6261646775792e636f6d')

(U//FOUO) Endpoint IP

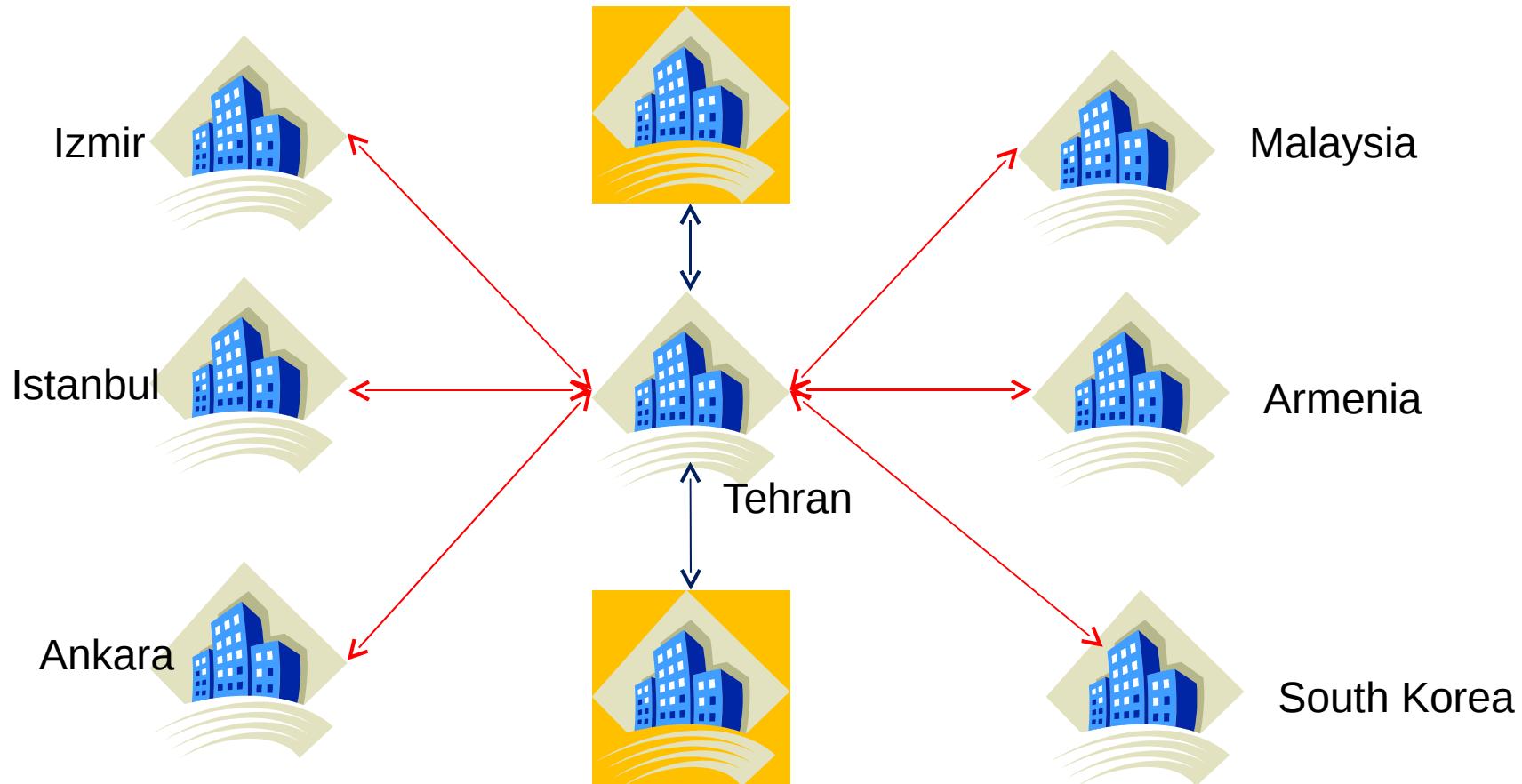
Search

- ⇒ (TS//SI//REL)Query each IP in TOYGRIPPE separately
 - Try to determine the importance of the connections
 - Note other VPN connections: all IPs are important until proven otherwise
- ⇒ (TS//SI//REL)Success: Discovered Iranian corporate intranet

(S//SI//REL) Building a VPN Intranet:



(S//SI//REL) Finding Suspicious VPN Connections



(TS//SI//REL) Two connections outside the target company

(S//SI//REL) Discovery of a Data Center

I had IP A, an endpoint IP from a router config...

And was looking for VPN connections to IP B, which I did not find...

....but in the process of looking, I found VPN connections to IP C in TOYGRIPPE....

(S//SI//REL) Discovery of a Data Center

...and when I did a follow on search in TOYGRIPPE for IP C....

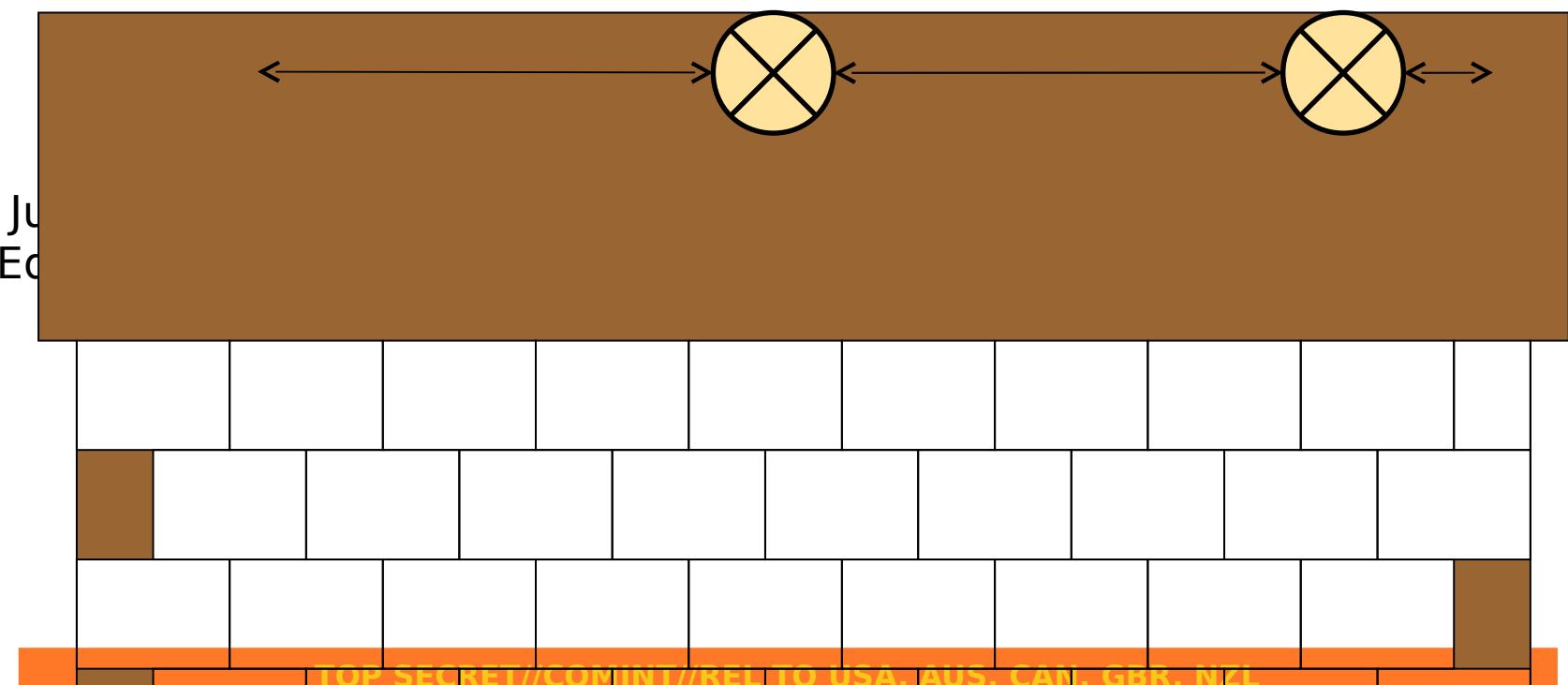
...I only found it only established VPN connections to IP A

Later discovered that IP C belonged to a data center in another country

(S//SI//REL) Search for other end of the point-to-point

- ☞ (S//SI//REL) What if you already have VPN endpoints from a GNOME report or a TOYGRIPPE search
- ☞ (S//SI//REL) Search for that IP in the DISCROUTE VPN report GUI - you don't find it
- ☞ (S//SI//REL) Try to search for the other end of what would be a point-to-point connection in DISCROUTE to find the customer edge router
- ☞ (S//SI//REL) END GOAL: find more information about the network

(S//SI//REL) Customer Edge Routers



(U//FOUO) NKB and RONIN

(S//SI//REL) NKB is NSA's Network Knowledge Base delivering target communications' DNI and enrichment data

(S//SI//REL) RONIN is a device characterization database and one of the enrichments to NKB

(U//FOUO) NKB

- ⇒ (S//SI//REL) RONIN data
 - ⇒ Server Analytics: VPN identified through application layer information in ASDF
 - ⇒ Wiki: VPN Metadata in ASDF
 - ⇒ VPN Analytics: endpoint in TOYGRIPPE
 - ⇒ Router Config: new descriptive information coming soon to include tunnel & VPN information for IPs
 - ⇒ Example: Kenya VPN IP [REDACTED]

(TS//SI//REL) NKB Search for [REDACTED]

Device Details

NKB: Home NKB: Results

Interface:ROUTER	IP ROUTE:Routed By	0
Service Interface:ROUTER		0
Hardware Interface:ROUTER	fast ethernet:IP	0
Service Interface: SERVER	vpn:IKEv1	vpn:IKEv1
Service Interface: SERVER	VPN:Cisco	VPN:Cisco
Hardware Interface:ROUTER	fast ethernet:IP	
Hardware Interface:ROUTER	unknown:IP	
Hardware Interface:ROUTER	unknown:IP	

DataSource	Service/Device	Type	Properties	Comments	Last Seen
RONIN	Hardware Interface:ROUTER	fast ethernet:IP	count=1 source=Router Config IP=[REDACTED]	[REDACTED] is serviced by interface "FastEthernet3" on the Cisco router named "pnbo192", model "c870", with netmask [REDACTED] and description "— To DSL provider". (Query DISCOROUTE)	2011-Aug-10
RONIN	Hardware Interface:ROUTER	fast ethernet:IP	count=5 source=Router Config IP=[REDACTED]	[REDACTED] is serviced by interface "FastEthernet4" on the Cisco router named "pnbo192", model "c870", with netmask [REDACTED] and description "— To DSL provider". (Query DISCOROUTE)	2011-Oct-12
RONIN	Hardware Interface:ROUTER	unknown:IP	count=1 source=Router Config IP=[REDACTED]	[REDACTED] is serviced by interface "FastEther.....N...." on the Cisco router named "pnbo192", model "c870", with netmask [REDACTED] and description "— To DSL provider". (Query DISCOROUTE)	2011-Oct-11
RONIN	Hardware Interface:ROUTER	unknown:IP	count=1 source=Router Config IP=[REDACTED]	[REDACTED] is serviced by interface "FastEther.....N....net4" on the Cisco router named "pnbo192", model "c870", with netmask [REDACTED] and description "— To DSL provider". (Query DISCOROUTE)	2011-Oct-13
RONIN	Service Interface:ROUTER	IP ROUTE:Routed By	count=1 source=Router Config IP=[REDACTED]	[REDACTED] was seen in a static route with a subnet [REDACTED] on router "BP_AGG01".	2011-Sep-12
RONIN	Hardware Interface:ROUTER	fast ethernet:IP	count=1 source=Router Config IP=[REDACTED]	41.206.52.139/32 was found as the IP for interface "FastEthernet3" on the Cisco router named "pnbo192"	count=50 source=SERVER_ANALYTIC IP=[REDACTED]
RONIN	Service Interface: SERVER	vpn:IKEv1	count=50 source=SERVER_ANALYTIC IP=[REDACTED]	vpn:IKEv1	count=195 source=UDN_Analytic IP=[REDACTED]
RONIN	Service Interface: SERVER	VPN:Cisco	count=195 source=VPN_Analytic IP=[REDACTED]	VPN:Cisco	

Done

(U//FOUO) GN ETWORK

GNOME

(S//SI//REL) Tool used to extract and correlate information from a variety of NAC, SSG, SSO, NTOC and other metadata databases



(S//SI//REL) Keep an Eye on the Entire Netblock

- ☞ (S//SI//REL) Multiple VPNs for one target
 - ⇒ different purposes
 - ⇒ different clients



(S//SI//REL) GNOME Task: Private IP VPNs

- ⇒ (S//SI//REL) Find a public IP associated with your private IP
 - ⇒ Loopback IP
 - ⇒ Another interface IP
- ⇒ (S//SI//REL) Use those for your GNOME report and look for your private IP on the same link
- ⇒ (S//SI//REL) Data presented in the VPN tab in GNOME report is limited



(U//FOUO) Network Patterns...

(S//SI//REL) IP Patterns

- ⇒ (S//SI//REL) Admins are people -- lean towards predictability in assignment of IPs to make their job easier
- ⇒ (S//SI//REL) IP or a combination of the octets could be an indication of:
 - ⇒ network provider
 - ⇒ location
 - ⇒ specific purpose in the network

(S//SI//REL) Example #1:Private IP VPN

Network Patterns

- ⇒ (S//SI//REL) Client side of the VPN: [REDACTED]
 - Second octet indicated the network provider
 - 20 = network provider #1
 - 21 = network provider #2
 - Second and third octet = country
 - 20.30 and 21.30 were the same country but different providers
 - 40 = individual target entity in that country
- ⇒ (S//SI//REL) Server side of the VPN: [REDACTED]
 - Second octet indicated network provider
 - 51= network provider #1
 - 52 = network provider #2

(S//SI//REL) Example #2:Network Patterns

(S//SI//REL) Public IP VPN: [REDACTED].#

- Third octet = country location of this IP (three possible)
- Fourth octet= country location of the other side of the VPN connection

Analyzed the opposite side of this /24 and identified the country for 167 4th octet values (out of 209) □ when this public IP connects to a private IP we know the country location of the private IP.

(U//FOUO) Final Thoughts...

- ⇒ (S//SI//REL) Just because you don't get results doesn't mean the answer isn't there
 - ⇒ If you're looking for a connection from A to B and don't find it, then maybe you need to look for one from A to C to B
- ⇒ (S//SI//REL) Try the query a different way
 - ⇒ Widen the search either by wildcarding (if permitted) or by selecting a different drop-down option
 - ⇒ Enter information in a different field

(U//FOUO)Final Thoughts...

- ⇒ (S//SI//REL) All IPs are important until proven otherwise
 - ⇒ They all serve a purpose and belong to a device
 - ⇒ Make note of what you find even if you don't know at the time what it means
- ⇒ (S//SI//REL) Search for data even if results are unlikely
- ⇒ (S//SI//REL) Don't necessarily discard dated information

(U//FOUO) Final Thoughts...

- ⇒ (U//FOUO) Understand the data that you are searching and what the fields in the GUI are searching for
- ⇒ (U//FOUO) Take an iterative approach: start searches wide, then narrow them down, then widen back out again
- ⇒ (S//SI//REL) Bounce between the different databases and use the tools for every aspect of your network analysis



(S//SI//REL) VPN SIGDEV: Build the network knowledge...

- ⇒ (TS//SI//REL) Dig beyond paired collection, PSKs and persistence
- ⇒ (S//SI//REL) Discovery of the inner IPs of the VPN is possible in ways other than decryption
- ⇒ (S//SI//REL) Investigate device IPs
- ⇒ (U//FOUO) Look for patterns
- ⇒ (S//SI//REL) Discover the ‘N’ of your VPN



(U//FOUO) Questions?



SSG21 Net Pursuit
Network Analysis Center

(S//SI//REL)
Simplifying and
Automating VPN
SIGDEV

SSG22

Network Analysis Center



(U//FOUO) The Ultimate Goals

- ⇒ (S//SI//REL) Integrate VPN information into mainstream analytic tools and knowledge bases.
- ⇒ (S//SI//REL) Give analysts the ability to discover, develop, and track known targets using VPNs.
- ⇒ (S//SI//REL) Give analysts the ability to discover new targets using VPNs.



(U//FOUO) The Start . . .

- ⇒ (S//SI//REL) Develop new corporate VPN tool (DARKSUNRISE).
 - ⇒ Joint collaboration between CES and the NAC.
 - ⇒ Take advantage of cloud architecture.
 - ⇒ Strive to meet the needs of the entire VPN community.



(U//FOUO) To The Cloud!

- (S//SI//REL) Data stored in MDR-2, the corporate metadata repository.
 - Stores one year of DNI metadata.
 - Enables filtering, aggregating, and transforming large datasets quickly.
 - Manage high data volumes.
 - Answer VPN questions efficiently and easily.



(S//SI//REL) What are Some of the Needs of the VPN SIGDEV Community?

(S//SI//REL) Answer VPN SIGDEV questions quickly.

- ⇒ (S//SI//REL) Allow SIGDEVers to spend time analyzing data instead of gathering and processing the data first.
- ⇒ (S//SI//REL) Make VPN SIGDEV more widely understood by simplifying and automating the SIGDEV process.
- ⇒ (S//SI//REL) Robust Structure
 - ⇒ Allow for multiple VPN and network encryption
 - ⇒ pAdtowoffer incorporation of new analytics.

(S//SI//REL)

What are Some of the Questions?

- » (S//SI//REL) Basic Questions
 - » Is my target using a VPN?
 - » What are all of the VPNs from country BadGuyLand?
 - » Tell me all of the VPNs where domain = sita*.
 - » Tell me all of the VPNs where the vendor ID = Cisco.

(S//SI//REL)

What are Some of the Questions?



- (S//SI//REL) Specialized Questions
 - » What are all of the VPNs that are bi-directional?
 - » What are all of the VPNs that are paired?
 - » Tell me all of the VPNs (and how many) that a particular VPN talks to (persistent hubs/centrality).
 - » What are all of the VPNs that are of interest (via Target Network Service)?
 - » What VPNs are associated to a router config?
 - » What are all of the VPNs that are persistent?
 - » For which VPNs do we have a PSK?

(S//SI//REL)

What are Some of the Questions?

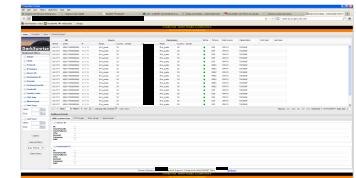


(S//SI//REL)

- ⇒ What are all of the VPNs that are bi-directional, persistent, and of interest?
- ⇒ What are all of the VPNs that are paired, persistent, and for which we have a PSK?
- ⇒ What are all of the VPNs from country BadGuyLand that are paired, associated to a router config, and of interest?

(U//FOUO) DARKSUNRISE

- ☞ (U//FOUO) This is a prototype GUI.
- ☞ (U//FOUO) Comingg Fall 2012



(S//SI//REL) DARKSUNRISE

Mozilla Firefox

File Edit View Bookmarks Tools Help

DNI Presenter - index TOYGRIPPE XKEYSCORE dsridge

R RoyalNet *Prototype* Free Form BLACKPEARL - WikiInfo

DYNAMIC PAGE - HIGHEST POSSIBLE CLASSIFICATION IS
TOP SECRET//COMINT//TK//NOFORN

Main Centrality Stats General Queries

SRI

SRI	Source				Destination				BiDir...	Protocol	Data Source	Classification	First Seen	Last Seen
SIGAD	CASN	IP	Realm	Country	IP	Realm	Country	Domain						
DS-200B	PK1S011	[REDACTED]	IPv4_public	SE	[REDACTED]	IPv4_public	PK	[REDACTED]	●	IPSEC	VPN-TU	TS//SI//REL TO USA...		
DS-200B	PK1S011	[REDACTED]	IPv4_public	RO	[REDACTED]	IPv4_public	PK	[REDACTED]	●	IPSEC	VPN-TU	TS//SI//REL TO USA...		
DS-200B	PK1S011	[REDACTED]	IPv4_public	RO	[REDACTED]	IPv4_public	PK	[REDACTED]	●	IPSEC	VPN-TU	TS//SI//REL TO USA...		
DS-200B	PK1S011	[REDACTED]	IPv4_public	TR	[REDACTED]	IPv4_public	PK	[REDACTED]	●	IPSEC	VPN-TU	TS//SI//REL TO USA...		
DS-200B	PK1S011	[REDACTED]	IPv4_public	TR	[REDACTED]	IPv4_public	PK	[REDACTED]	●	IPSEC	VPN-TU	TS//SI//REL TO USA...		
DS-200B	PK1S011	[REDACTED]	IPv4_public	AE	[REDACTED]	IPv4_public	AF	[REDACTED]	●	IPSEC	VPN-TU	TS//SI//REL TO USA...		
DS-200B	PK1S011	[REDACTED]	IPv4_public	AE	[REDACTED]	IPv4_public	PK	[REDACTED]	●	IPSEC	VPN-TU	TS//SI//REL TO USA...		
DS-200B	PK1S011	[REDACTED]	IPv4_public	AE	[REDACTED]	IPv4_public	PK	[REDACTED]	●	IPSEC	VPN-TU	TS//SI//REL TO USA...		
DS-200B	PK1S011	[REDACTED]	IPv4_public	CZ	[REDACTED]	IPv4_public	PK	[REDACTED]	●	IPSEC	VPN-TU	TS//SI//REL TO USA...		
DS-200B	PK1S011	[REDACTED]	IPv4_public	CZ	[REDACTED]	IPv4_public	PK	[REDACTED]	●	IPSEC	VPN-TU	TS//SI//REL TO USA...		
DS-200B	PK1S011	[REDACTED]	IPv4_public	AE	[REDACTED]	IPv4_public	AF	[REDACTED]	●	IPSEC	VPN-TU	TS//SI//REL TO USA...		
DS-200B	PK1S011	[REDACTED]	IPv4_public	TR	[REDACTED]	IPv4_public	PK	[REDACTED]	●	IPSEC	VPN-TU	TS//SI//REL TO USA...		
DS-200B	PK1S011	[REDACTED]	IPv4_public	NL	[REDACTED]	IPv4_public	PK	[REDACTED]	●	IPSEC	VPN-TU	TS//SI//REL TO USA...		
DS-200B	PK1S011	[REDACTED]	IPv4_public	US	[REDACTED]	IPv4_public	PK	[REDACTED]	●	IPSEC	VPN-TU	TS//SI//REL TO USA...		

Page 1 of 3 | Checking TNS.Finished! Finished! | Clear Filters Reports: csv html xls ren ivml | Displaying 1 - 100 of 236 | Page Size 100

Shadownet Filters

- SIGAD: [REDACTED]
- CASN: [REDACTED]
- Protocol: [REDACTED]
- IP Ranges: [REDACTED]
- Source IP: [REDACTED]
- Destination IP: [REDACTED]
- Domain: [REDACTED]
- ExchangeTypeId: [REDACTED]
- VendorId: [REDACTED]
- Country Code: [REDACTED]
- FVEY Only: [REDACTED]
- BiDirectional: [REDACTED]
- First Seen:
- Start: [REDACTED] End: [REDACTED]
- Last Seen:
- Start: [REDACTED] End: [REDACTED]

Drilldown/Details

NKB Location Data PPTP Details IPSec Details VipNet Details

Source IP

IP: [REDACTED]
 CountryCode: RO
 CountryName: ROMANIA
 City: BUCHAREST
 Domain: ROMTELECOM.NET
 Company: ROMTELECOM DATA NETWORK
 ASN: 9050

Destination IP

IP: [REDACTED]
 CountryCode: PK
 CountryName: PAKISTAN
 City: KARACHI
 Domain: TW1.COM
 Company: GRUPM
 ASN: 38193

Submit
 Clear all Filters
 Gray Theme
 Clear Cache

Content Steward [REDACTED] General Support: Contact the SHADOWNET Team [REDACTED] feedback

DYNAMIC PAGE - HIGHEST POSSIBLE CLASSIFICATION IS

TOP SECRET//COMINT//TK//NOFORN

(TS//SI//REL) The NKB Location Data Drilldown

Mozilla Firefox

File Edit View History Bookmarks Tools Help

DNI Presenter - index TOYGRIPPE XKEYSCORE dsridge

RoyalNet Prototype*

BLAKEYELAW TRAP

Google

DYNAMIC PAGE - HIGHEST POSSIBLE CLASSIFICATION IS
TOP SECRET//COMINT//TK//NOFORN

Main Centrality Stats General Queries

DarkSunrise

Shadownet Filters

- SIGAD:
- CASN:
- Protocol:
- IP Ranges:
- Source IP:
- Destination IP:
- Domain:
- ExchangeTypeId:
- VendorId:
- Country Code:
- FVEY Only:
- BiDirectional:
- First Seen: Start: End:
- Last Seen: Start: End:

Page 1 of 3 | Checking TNS.Finished! | Clear Filters

SRI		Source				Destination				BiDir...	Protocol	Data Source	Classification	First Seen	Last Seen	
SIGAD	CASN	IP	Realm	Country	Domain	IP	Realm	Country	Domain							
DS-200B	PK1S011	[REDACTED]	IPv4_public	SE		[REDACTED]	IPv4_public	PK	[REDACTED]	●	IPSEC	VPN-TU	TS//SI//REL TO USA...			
DS-200B	PK1S011	[REDACTED]	IPv4_public	RO		[REDACTED]	IPv4_public	PK	[REDACTED]	●	IPSEC	VPN-TU	TS//SI//REL TO USA...			
DS-200B	PK1S011	[REDACTED]	IPv4_public	RO		[REDACTED]	IPv4_public	PK	[REDACTED]	●	IPSEC	VPN-TU	TS//SI//REL TO USA...			
DS-200B	PK1S011	[REDACTED]	IPv4_public	TR		[REDACTED]	IPv4_public	PK	[REDACTED]	●	IPSEC	VPN-TU	TS//SI//REL TO USA...			
DS-200B	PK1S011	[REDACTED]	IPv4_public	TR		[REDACTED]	IPv4_public	PK	[REDACTED]	●	IPSEC	VPN-TU	TS//SI//REL TO USA...			
DS-200B	PK1S011	[REDACTED]	IPv4_public	AE		[REDACTED]	IPv4_public	AF	[REDACTED]	●	IPSEC	VPN-TU	TS//SI//REL TO USA...			
DS-200B	PK1S011	[REDACTED]	IPv4_public	AE		[REDACTED]	IPv4_public	PK	[REDACTED]	●	IPSEC	VPN-TU	TS//SI//REL TO USA...			
DS-200B	PK1S011	[REDACTED]	IPv4_public	AE		[REDACTED]	IPv4_public	PK	[REDACTED]	●	IPSEC	VPN-TU	TS//SI//REL TO USA...			
DS-200B	PK1S011	[REDACTED]	IPv4_public	CZ		[REDACTED]	IPv4_public	PK	[REDACTED]	●	IPSEC	VPN-TU	TS//SI//REL TO USA...			
DS-200B	PK1S011	[REDACTED]	IPv4_public	CZ		[REDACTED]	IPv4_public	PK	[REDACTED]	●	IPSEC	VPN-TU	TS//SI//REL TO USA...			
DS-200B	PK1S011	[REDACTED]	IPv4_public	AE		[REDACTED]	IPv4_public	AF	[REDACTED]	●	IPSEC	VPN-TU	TS//SI//REL TO USA...			
DS-200B	PK1S011	[REDACTED]	IPv4_public	AE		[REDACTED]	IPv4_public	PK	[REDACTED]	●	IPSEC	VPN-TU	TS//SI//REL TO USA...			
DS-200B	PK1S011	[REDACTED]	IPv4_public	TR		[REDACTED]	IPv4_public	PK	[REDACTED]	●	IPSEC	VPN-TU	TS//SI//REL TO USA...			
DS-200B	PK1S011	[REDACTED]	IPv4_public	NL		[REDACTED]	IPv4_public	PK	[REDACTED]	●	IPSEC	VPN-TU	TS//SI//REL TO USA...			
DS-200B	PK1S011	[REDACTED]	IPv4_public	US		[REDACTED]	IPv4_public	PK	[REDACTED]	●	IPSEC	VPN-TU	TS//SI//REL TO USA...			

Reports: csv html xls ren ivml | Displaying 1 - 100 of 236 | Page Size 100

Drilldown/Details

NKB Location Data PPTP Details IPSec Details VipNet Details

Source IP

IP: [REDACTED]
 CountryCode: RO
 CountryName: ROMANIA
 City: BUCHAREST
 Domain: ROMTELECOM.NET
 Company: ROMTELECOM DATA NETWORK
 ASN: 9050

Submit Clear all Filters Gray Theme Clear Cache

Destination IP

IP: [REDACTED]
 CountryCode: PK
 CountryName: PAKISTAN
 City: KARACHI
 Domain: TV1.COM
 Company: GRUPM
 ASN: 38193

Content Steward [REDACTED] General Support: Contact the SHADOWNET Team [REDACTED] feedback

(TS//SI//REL) The IPSec Details Drilldown

SHADOWNET

Shadownet Filters

- SIGAD: CASH
- CASIN: [REDACTED]
- Protocol: IPsec
- IP Ranges: [REDACTED]
- Source IP: [REDACTED]
- Destination IP: [REDACTED]
- ExchangeTypeIds: [REDACTED]
- VendorId: [REDACTED]
- Country Code: PK
- FVEY Only:
- BiDirectional:
- Apply Filters and Refresh Data:
- Clear all Filters:
- Blue Theme:
- Clear Cache:

Drilldown/Details

- NIDS/Log Data: PPTP Details:
- IPSec Details:
- VipNet Details:

IPSec

Encryption Alg ID:	7	Encryption Algorithm:	AES-CBC	Group ID:	Private Attr Type:
Authentication Method Id:	3	Authentication Method:	RSA Signature		
Ike Vendor Ids:	[REDACTED]	Vendor ID: 214ca-ffaffa732d6748e5303395ae83	VID Type: Vendor	Brand/Provider: Microsoft	Details/Version: Vista/Longhorn (AuthIP supported)
Exchange Type Ids:	[REDACTED]				
Exchange Type ID:	[REDACTED]				

Content Steward: [REDACTED] **General Support:** Contact the SHADOWNET Team **Feedback:** [REDACTED]

DYNAMIC PAGE - HIGHEST POSSIBLE CLASSIFICATION IS TOP SECRET//COMINT//REL TO USA, AUS, CAN, GBR, NZL

SHADOWNET

Shadownet Filters

- SIGAD: CASH
- CASIN: [REDACTED]
- Protocol: IPsec
- IP Ranges: [REDACTED]
- Source IP: [REDACTED]
- Destination IP: [REDACTED]
- ExchangeTypeIds: [REDACTED]
- VendorId: [REDACTED]
- Country Code: PK
- FVEY Only:
- BiDirectional:
- Apply Filters and Refresh Data:
- Clear all Filters:
- Blue Theme:
- Clear Cache:

Drilldown/Details

- NIDS/Log Data: PPTP Details:
- IPSec Details:
- VipNet Details:

IPSec

Encryption Alg ID:	7	Encryption Algorithm:	AES-CBC	Group ID:	Private Attr Type:
Authentication Method Id:	3	Authentication Method:	RSA Signature		
Ike Vendor Ids:	[REDACTED]	Vendor ID: 214ca-ffaffa732d6748e5303395ae83	VID Type: Vendor	Brand/Provider: Microsoft	Details/Version: Vista/Longhorn (AuthIP supported)
Exchange Type Ids:	[REDACTED]				
Exchange Type ID:	[REDACTED]				

Content Steward: [REDACTED] **General Support:** Contact the SHADOWNET Team **Feedback:** [REDACTED]

DYNAMIC PAGE - HIGHEST POSSIBLE CLASSIFICATION IS TOP SECRET//COMINT//REL TO USA, AUS, CAN, GBR, NZL

(TS//SI//REL)

Automatic Identification of Bi-directional VPNs

The screenshot displays a web-based application for network analysis, specifically for identifying bi-directional VPN connections. The interface is organized into several sections:

- Left Sidebar:** Contains filter panels for "SIGAD", "CASN", "Protocol", "IP Ranges", "Source IP", "Destination IP", and "Domain". It also includes sections for "ExchangeType", "VendorID", "Country Code", and checkboxes for "FVEY Only" and "BiDirectional".
- Main Content Area:** Features two large tables side-by-side.
 - Source Table:** Columns include SRI, SIGAD, CASN, IP, Realm, Country, Domain, and ID.
 - Destination Table:** Columns include IP, Realm, Country, Domain, and ID.Both tables show multiple rows of data, with several entries circled in red.
- Bottom Section:** Provides detailed information for selected source and destination IP addresses. It includes fields for "Source IP" (IP: 52.18.10.11, Country: SG, City: SINGAPORE, Domain: LHLACCPAC.COM, Company: STARHUB INTERNET PTE LTD, ASN: 9874) and "Destination IP" (IP: 103.24.131.11, Country: PK, City: ISLAMABAD, Domain: MICRONET BROADBAND (PVT) LTD, ASN: 23674).

(TS//SI//REL)

Automatic Identification of

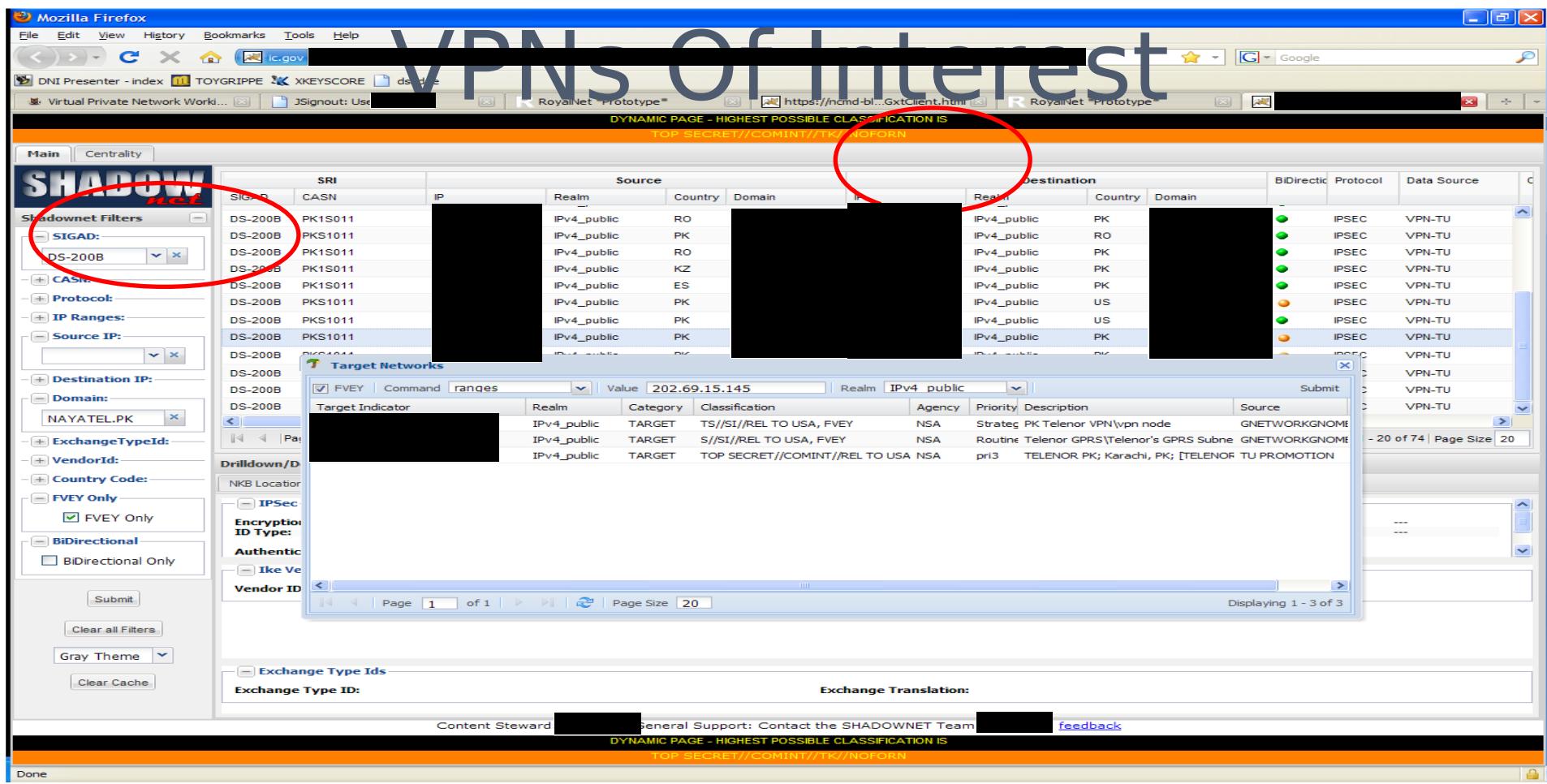
VPNs of Interest

The screenshot shows a Mozilla Firefox browser window displaying the SHADOWNET application. The main interface has a blue header bar with tabs like 'Main' and 'Centrality'. On the left, there's a sidebar with 'SHADOW' branding and various filters: 'SIGAD', 'CASN', 'Protocol', 'IP Ranges', 'Source IP', 'Destination IP', 'Domain', 'ExchangeType Id', 'Vendor Id', 'Country Code', 'FVEY Only' (which is checked), 'BiDirectional' (which is checked), and 'BiDirectional Only'. Below these filters are buttons for 'Submit', 'Clear all Filters', 'Gray Theme', and 'Clear Cache'. The main content area contains two tables. The top table is titled 'SRI' and lists connections between 'Source' and 'Destination' networks. The bottom table is titled 'Drilldown/Details' and provides more specific information about an selected connection, including 'Encryption Alg ID', 'Authentication Method Id', 'IKE Vendor Ids', and 'Exchange Type Ids'. A red circle highlights the 'Group ID: Private Attr Type:' field in the Drilldown/Details section. At the bottom of the page, there are links for 'Content Steward', 'General Support', 'Contact the SHADOWNET Team', 'feedback', and classification information: 'DYNAMIC PAGE - HIGHEST POSSIBLE CLASSIFICATION IS TOP SECRET//COMINT//TK//NOFORN'.

- (S//SI//REL) The icon means this record hits against the Target Network Service (TNS).

(TS//SI//REL)

Automatic Identification of





(S//SI//REL)

The Centrality Tab

DYNAMIC PAGE - HIGHEST POSSIBLE CLASSIFICATION IS
TOP SECRET//COMINT//TK//NOFORN

Address	Realm	Centrality
[REDACTED]	IPv4_public	2

- (S//SI//REL) Find all VPNs that talk to a base VPN.
 - Discover persistent hubs.
 - Can continue chaining outwards.

(S//SI//REL) **The Centrality Tab**

DYNAMIC PAGE - HIGHEST POSSIBLE CLASSIFICATION IS
TOP SECRET//COMINT//REL//NOFORN

Main Centrality Stats General Queries

Centrality Filters

IP Ranges: [REDACTED] Address: [REDACTED] Realm: IPv4_public Centrality: 2

Submit

Results

IP Range	Address	Realm	Centrality
[REDACTED]	[REDACTED]	IPv4_public	2

Displaying 1 - 1 of 1 | Page Size 30

(S//SI//REL)

The Centrality Tab

DYNAMIC PAGE - HIGHEST POSSIBLE CLASSIFICATION IS
TOP SECRET//COMINT//REL TO USA, AUS, CAN, GBR, NZL

Main | Centrality | Stats | General Queries |

Centrality Filters

IP Ranges	Address	Realm	Centrality
[REDACTED]	[REDACTED]	[REDACTED]	2

Submit

Main | Centrality | Stats | General Queries |

Centrality Filters

IP Ranges	Address	Realm	Centrality
[REDACTED]	[REDACTED]	[REDACTED]	2

Partners of [REDACTED]

IP Range	Realm	Centrality
[REDACTED]	[REDACTED]	3
[REDACTED]	[REDACTED]	3

Partners of [REDACTED]

IP Range	Realm	Centrality
[REDACTED]	[REDACTED]	7
[REDACTED]	[REDACTED]	3
[REDACTED]	[REDACTED]	2

Page 1 of 1 | Page Size 30 | Displaying 1 - 1 of 1 | Page Size 30

Content Steward [REDACTED] General Support: Contact the SHADOWNET Team [REDACTED] feedback

DYNAMIC PAGE - HIGHEST POSSIBLE CLASSIFICATION IS
TOP SECRET//COMINT//REL TO USA, AUS, CAN, GBR, NZL

(S//SI//REL) The Centrality Tab

DYNAMIC PAGE - HIGHEST POSSIBLE CLASSIFICATION IS
TOP SECRET//COMINT//TQ//NOFORN

DYNAMIC PAGE - HIGHEST POSSIBLE CLASSIFICATION IS
TOP SECRET//COMINT//TQ//NOFORN

Address	Realm	Centrality
[REDACTED]	IPv4_public	2

Address	Realm	Centrality
[REDACTED]	IPv4_public	3
[REDACTED]	IPv4_public	3

Address	Realm	Centrality
[REDACTED]	IPv4_public	7
[REDACTED]	IPv4_public	3
[REDACTED]	IPv4_public	2

Address	Realm	Centrality
[REDACTED]	IPv4_public	4
[REDACTED]	IPv4_public	3
[REDACTED]	IPv4_public	1

Content Steward [REDACTED] General Support: Contact the SHADONET Team [REDACTED] feedback
DYNAMIC PAGE - HIGHEST POSSIBLE CLASSIFICATION IS
TOP SECRET//COMINT//TQ//NOFORN

(S//SI//REL) The Centrality Tab

Two screenshots of a web application interface are shown side-by-side. Both screenshots feature a top navigation bar with tabs: Main, Centrality, Stats, and General Queries. The 'Centrality' tab is active in both.

The left screenshot shows a single table under the 'Centrality' tab. It has columns: Address, Realm, and Centrality. One row is visible, showing an IP range (IPv4_public) with a Centrality value of 2.

Address	Realm	Centrality
IPv4_public		2

The right screenshot shows four separate tables, each titled 'Partners of [REDACTED]'. Each table has columns: Address, Realm, and Centrality. The first table has two rows: IPv4_public (Centrality 3) and IPv4_public (Centrality 3). The second table has three rows: IPv4_public (Centrality 7), IPv4_public (Centrality 3), and IPv4_public (Centrality 2). The third table has five rows: IPv4_public (Centrality 4), IPv4_public (Centrality 3), IPv4_public (Centrality 3), IPv4_public (Centrality 3), and IPv4_public (Centrality 1). The fourth table has three rows: IPv4_public (Centrality 31), IPv4_public (Centrality 29), and IPv4_public (Centrality 7).

Address	Realm	Centrality
IPv4_public		3
IPv4_public		3

Address	Realm	Centrality
IPv4_public		7
IPv4_public		3
IPv4_public		2

Address	Realm	Centrality
IPv4_public		4
IPv4_public		3
IPv4_public		3
IPv4_public		3
IPv4_public		1

Address	Realm	Centrality
IPv4_public		31
IPv4_public		29
IPv4_public		7

At the bottom of the right screenshot, there are pagination controls: Page 1 of 1, Clear Filters, and a note indicating 'Displaying 1 - 1 of 1 | Page Size 30'. The footer also includes a Content Steward, General Support contact information, and a feedback link.



(U//FOUO)

The Metrics Tab

- (S//SI//REL) Count distinct VPN records, grouping them by one or more of the following attributes:
 - SIGAD
 - Source
 - VPN Type
 - Case Notation
 - Date



(U//FOUO) The Metrics Tab: One Example

SIGAD X

Metrics Tab: One Example

This screenshot shows two side-by-side views of a metrics tab interface, likely from a web-based reporting system. Both views display data for 'SIGAD' (System Information Group Analysis Detail) and 'VPN Type'.

Left View:

- Row Headers:** SIGAD
- Column Headers:** SIGAD, ESP, IKE_ESP_NAT..., IKEv1, IKEv2, IPSEC, PPTP, RDP, SSH, VIPNET, Total
- Data:**

SIGAD	ESP	IKE_ESP_NAT...	IKEv1	IKEv2	IPSEC	PPTP	RDP	SSH	VIPNET	Total
US-J759A	60677		7							60684
DS-2098	31931			64						31995
US-J790	238									238
USD-1001TEC	10793									10793
US-J799			1							1
US-3141B	551	45978			144688					5341 199558
UKC-1155W			24							24
US-J790			12							12
US-J759	4919									4919
US-3140	1	1958				144688				1957
	109110									307181

Right View:

- Row Headers:** SIGAD
- Column Headers:** SIGAD, ESP, IKE_ESP_NAT..., IKEv1, IKEv2, IPSEC, PPTP, RDP, SSH, VIPNET, Total
- Data:**

SIGAD	ESP	IKE_ESP_NAT...	IKEv1	IKEv2	IPSEC	PPTP	RDP	SSH	VIPNET	Total
US-J799			1							1
DS-2098	31931			64						31995
US-J790	238									238
USD-1001TEC	10793									10793
US-3141B	551	45978			144688					5341 199558
UKC-1155W			24							24
US-J790			12							12
US-J759	4919									4919
US-3140	1	1958				144688				1957
	109110									307181

Bottom Navigation:

- Content Steward [REDACTED] General Support: Contact the SHADONET Team [REDACTED] feedback
- DYNAMIC PAGE - HIGHEST POSSIBLE CLASSIFICATION IS (TOP SECRET//COMINT//REL TO USA, AUS, CAN, GBR, NZL)

- (TS//SI//REL) Total number of VPN type per SIGAD.



(U//FOUO) The Ultimate Goals

- ⇒ (S//SI//REL) Integrate VPN information into mainstream analytic tools and knowledge bases.
- ⇒ (S//SI//REL) Give analysts the ability to discover, develop, and track known targets using VPNs.
- ⇒ (S//SI//REL) Give analysts the ability to discover new targets using VPNs.

(U//FOUO)

Questions?



SSG22
Network Analysis Center